基于虚拟机迁移的 DoS 攻击防御方法 *

张 淼，季新生，刘文彦，杨 超，霍树民，程国振

(国家数字交换系统工程技术研究中心，郑州 450002)

摘 要：利用云计算资源共享的特性，攻击者可以通过不停消耗带宽资源，使得同一物理主机上的其他用户无法接受正常服务，造成拒绝服务（denial of service，DoS）攻击。这种攻击区别于传统网络体系中的 DoS 攻击，因此难以应用传统防御方法解决。针对这一问题，提出一种基于虚拟机迁移的 DoS 攻击防御方法，通过选择迁移目标、设计触发机制和选择迁移目的地，形成迅速减轻 DoS 攻击影响的虚拟机迁移策略。实验结果表明，针对攻击者的不同攻击方式，该方法均可有效地快速防御 DoS 攻击，保证云服务的正常运行。相比其他策略，所提方法在迁移开销上略有增加，但防御效果明显，可行性更高。

关键词：云计算；DoS 攻击；虚拟机迁移

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.01.0095

Defensive method against DoS attack based on virtual machine migration

Zhang Miao, Ji Xinsheng, Liu Wenyan, Yang Chao, Huo Shumin, Chen Guozhen

(*National Digital Switching Engineering & Technological R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: By utilizing the characteristics of resource sharing in cloud computing, attackers can launch DoS attack by constantly consuming bandwidth resources so that other users on the same physical host can not receive normal services. This attack mode is different from the DoS attack in traditional network system, so it is difficult to apply traditional defense method to solve it. To solve this problem, this paper proposes a DoS attack defense method based on virtual machine migration. By selecting the migration target, designing the triggering mechanism and selecting the migration destination, a virtual machine migration strategy is proposed to mitigate the impact of DoS attacks. The experimental results demonstrate that this method can effectively defend DoS attack and ensure the normal operation of cloud service whatever different attack methods that attackers may use. Compared with other methods, the proposed strategy leads a litter more migration cost, however, it's better in defense effect and feasibility.

Key words: cloud computing; DoS attack; virtual machine migration

0 引言

云计算中虚拟化技术可以实现对 CPU、存储等物理资源的池化，从而使得不同的用户可以共享这些资源。然而，这种模式也成为攻击者方便利用的漏洞。当不同用户的虚拟机运行于同一物理主机上时，攻击者可以利用侧信道、隐蔽信道等方式，窃取目标虚拟机的机密信息或探测其负载状态，这类攻击被称为共存攻击或同驻攻击[错误!未找到引用源。]。发起共存攻击的方式有多种，其中，恶意虚拟机利用网络通道发送无效数据或者利用漏洞不停占用底层资源，从而造成正常用户服务受到影响，形成一种云环境下特有的拒绝服务（DoS）攻击[错误!未找到引用源。]。这种攻击区别于传统网络中 DoS 的形式，但同样会对云平台的正常运行造成严重威胁。

传统网络体系中，DoS 或者 DDoS（distributed denial of service，分布式拒绝服务）攻击一般是由攻击者控制的僵尸网络，向攻击目标或服务持续地发送应用请求和攻击流量，降低目标服务可用性，增加用户运行的成本和开销。与之相比，云环境下的 DoS 攻击形式更加多样，如可以利用云计算的树形拓扑，造成带宽饥饿攻击；对采用 SDN 架构发起的控制层、数据层攻击等。而且按需服务的特点使得大规模僵尸网络更加容易

收稿日期：2018-01-08；**修回日期：**2018-03-23　**基金项目：**国家重点研发计划资助项目（2016YFB0800100，2016YFB0800101）；国家自然科学基金创新研究群体项目（61521003）；国家自然科学基金青年基金资助项目（61602509）；河南省科技攻关计划资助项目（172102210615）

作者简介：张淼（1994-），男，湖北孝感人，硕士，主要研究方向为网络安全防御（15537163512@163.com）；季新生（1968-），男，江苏南通人，教授，博导，主要研究方向为网络空间安全、无线通信等；刘文彦（1986-），男，河南鹿邑人，助理研究员，主要研究方向为网络空间防御和云安全；杨超（1990-），男，浙江衢州人，博士，主要研究方向为侧信道攻击防御等；霍树民（1985-），山西长治人，助理研究员，主要研究方向为网络空间安全；程国振（1986-），男，山东定陶人，助理研究员，主要研究方向为软件定义网络.

构建，资源共享的模式也让与目标相关联的用户数量增加，攻击面被扩大。云计算的很多特点成为了攻击者利用的漏洞，使得传统的防御方法很难在云环境中有效使用。

虚拟机迁移指的是将虚拟机从一个主机或存储位置移动到另一个主机或存储位置的过程，其中实时迁移（live migration）可以保证在服务不中断的情况下实现一种对用户透明的迁移，从而在负载均衡、在线维护等方面起到重要作用，得到了广泛的研究。由于云环境中的 DoS 攻击的主要威胁是影响虚拟机的正常服务，因此本文考虑利用虚拟机迁移技术，将虚拟机从遭受这种 DoS 攻击的主机上迁移到其他正常的主机上，使得服务可以正常运行，同时释放源主机上的带宽资源，缓解 DoS 攻击。

本文的攻防模型建立在基于 OpenStack 的云平台上，从是否具备信息获取能力和恶意流量能否调节两方面，将攻击者分为四种情形，针对不同的攻击形式，提出统一的虚拟机迁移策略，包括对虚拟机的选择、迁移的触发机制和迁移目的地。实验结果验证了所提方法的可行性和有效性。

1 相关研究

针对云环境中的 DoS 攻击，研究人员提出了一些不同的解决思路。Harkeerat 等人错误!未找到引用源。发现 EC2 平台下虚拟机与网络的流量都会经过 domain 0，因此提出一种博弈策略，通过设定防火墙的阈值来过滤恶意攻击者的流量，但是这种方法对正常用户超过阈值的流量也进行过滤，实用性较差。Qiao 等人[3]利用 SDN（software-defined networking，软件定义网络）网络控制和数据平面分离、流规则动态更新等特点，提出用 SDN 架构来探测并处理 DoS 攻击，然而 SDN 本身可能成为攻击的目标，且对于现有架构的修改使得这种方法难以大规模部署。Zhang 等人错误!未找到引用源。针对基于主机的 DoS 攻击，利用统计方法探测不同资源的利用率变化情况，来鉴定和阻止恶意虚拟机发起的内存、硬盘上的 DoS 攻击，这种防御方法可以有效解决特定条件下的攻击，但对其他类型的 DoS 攻击无法起到作用。

一直以来，虚拟机迁移的实用性得到了广泛的关注。一方面，利用虚拟机迁移，云服务提供商（cloud service provider,CSP）可以实现负载均衡、资源节约、在线维护等功能，提高资源利用率、保证服务质量；同时，随着网络安全的重要程度日益增强，利用虚拟机迁移保护用户数据隐私安全也成为一种研究方向。如 Moon 等人错误!未找到引用源。建立了云侧信道信息泄露的模型，利用迁移减小信息泄漏风险，但随着网络规模的扩大，迁移开销迅速增加。文献**错误!未找到引用源。**在此基础上，对虚拟机进行等级分类，提出开销节约的虚拟网映射和迁移策略。由于虚拟机迁移技术、机制等都已经较为成熟，因此将其应用于安全领域时，可以迅速发挥作用。然而到目前为止，未发现在防御 DoS 攻击上利用虚拟机迁移的研究，因此本文希望可以将虚拟机迁移的应用场景再次扩大，并启发其他研究人员应用动态防御思想解决云安全问题。

2 云平台模型

OpenStack 是一个开源的云计算管理平台，一般由控制节点、计算节点、网络节点和存储节点四个部分组成。其中控制节点和计算节点基本可以实现 OpenStack 的重要功能。控制节点负责对其余节点进行控制，主要包括了虚拟机的建立和迁移，以及网络资源的分配等；计算节点则负责虚拟机的运行。

如图 1 所示，三台物理服务器上分别安装了一个控制节点和两个计算节点。在计算节点上，虚拟机通过数据网络实现与内网和外网的连接；而控制节点通过管理网络与计算节点之间进行通信，向计算节点发送控制指令。值得注意的是，虚拟机的迁移也是通过管理网络实现的，即虚拟机内存、磁盘的迁移不会影响数据层的网络带宽。因此，迁移过程不会加重网络的负载，迁移完成后，还能缓解拥塞，使得网络重新提供正常的服务。

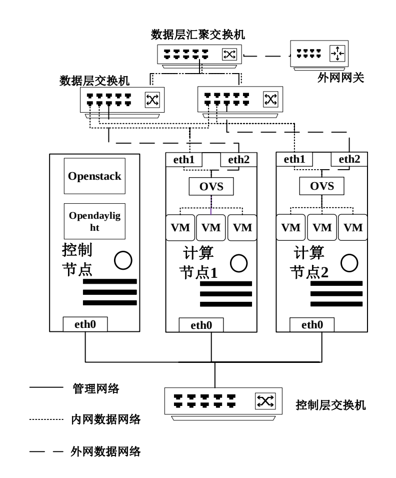


图 1 基于 OpenStack 的简易云架构模型

图 2 表示在一个物理主机上，虚拟机 1 为攻击者拥有，虚拟机 2 和 3 属于正常用户。当恶意攻击者不停发送大量的流量时（图 2 中 A 部分），会消耗主机上较多的带宽资源，从而使得虚拟交换机（图中 OVS，Open vSwitch）的上行链路产生拥塞（B 部分）。由于虚拟机与外部的通信都必须经过 OVS，因此当 OVS 链路的带宽需求超过其资源总量时，服务器上其他正常用户虚拟机的服务必然受到影响，即遭受 DoS 攻击。

显然，攻击者发起 DoS 攻击造成的影响，与主机上正常用户虚拟机的数量呈正相关的关系。极端情况下，若主机上仅存在攻击者，那么攻击行为不会对主机上的其他用户产生影响；而随着用户虚拟机数量的增加，只要网络发生拥塞，那么整个主机上的用户都会受到干扰。

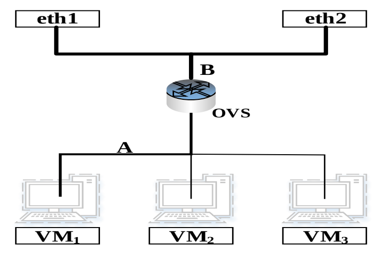


图 2 攻击者占用带宽资源造成 DoS 攻击

3　攻击者行为

云服务提供商在部署用户虚拟机时，会根据虚拟机的属性将其分配到适当的主机上，即虚拟机可利用的资源受到其类型的限制，且最大需求不会超过主机的承受能力。因此，在网络中出现剧增的流量时，提供商无法判断该虚拟机增加的流量来源于用户的正常需求或是攻击者的恶意行为。云计算这种按需分配的模式使得传统的入侵检测方法无法应用，因此，发生 DoS 攻击时，服务提供商难以对某一虚拟机进行限制，否则可能违反 SLA(service level agreements,服务水平协议)。

随着攻击手段的丰富，攻击者探测系统信息的能力也逐渐提高；而上文也提到，攻击者可以调节发送的恶意流量，进一步迷惑云服务提供商，保证攻击行为的持续性。因此，本文按照攻击者的信息（information）获取能力和对恶意流量是否自调节（adjustable），将其行为分为以下四种情形：a)可以获取主机资源信息，且自我调节攻击流量。攻击者有能力探测各主机上虚拟机的数量和资源利用情况，选择当前带宽需求量最大的主机进行攻击，在部署攻击虚拟机后，可以调节发送的攻击流量，使得云服务提供商无法判断其是否为恶意攻击者；b)没有信息获取能力，不具备流量调节能力。攻击者任意选择云平台中主机进行无差别的攻击，并让恶意虚拟机持续性发送相同的流量，从而迅速在该主机上形成 DoS 攻击；c)可以获取主机资源信息，不具备流量调节能力；d)没有信息获取能力，可自我调节攻击流量。将上述四种攻击者模型分别记为<*I*，*A*>，<*NI*，*NA*>，<*I*，*NA*>，<*NI*，*A*>。

4　防御 DoS 攻击的虚拟机迁移策略

本文利用虚拟机迁移来防御云平台中的 DoS 攻击，由于云环境中虚拟机数量多，且资源利用情况时刻在发生变化，迁移虚拟机时必须有相应的策略，才能在防御 DoS 攻击的同时，尽可能降低迁移开销。一般而言，虚拟机的迁移策略包括三个方面：择待迁移的虚拟机；设定迁移的触发条件，或选择迁移时刻；选择目的主机，将虚拟机从源主机迁移至目的主机上。本文分别设置如下迁移策略：

4.1　迁移虚拟机的选择

当发现某一主机产生网络拥塞时，首先需要选择从该主机上迁移出去的特定虚拟机。本小节提出一种虚拟机选择策略，每次迁移完成后，重新检测物理主机的网络状态，如果仍然处于拥塞，则继续选择剩余的虚拟机进行迁移，直到云平台能向用户提供正常的可靠服务。

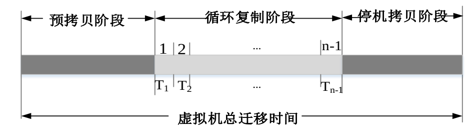


图 3　虚拟机预拷贝迁移的过程

由于在迁移过程中需要保证服务的连续性，一般对虚拟机进行实时在线迁移。目前最常用的方式是预拷贝迁移错误!未找到引用源。，即先将源虚拟机的内存复制到目的主机上，然后反复迭代拷贝内存脏页，直到内存小于一个阈值或者迭代次数达到设置的最大值为止。如上图 3 所示，令虚拟机的内存大小为 M，迁移过程中脏页率为 R，分配给迁移的可用带宽为 L。假设拷贝过程进行 n 轮，每轮数据传输量为 $V_i(0 \le i \le n)$，所用时间为 $T_i(0 \le i \le n)$。则第一轮中所有内存页都会被复制到目的主机上，即 $V_0 = M$。下一轮中，会将上一轮被修改的页面再次复制到目的主机。因此每轮的数据传输量为

$$V_i = R \cdot T_{i-1}, i > 0 \tag{1}$$

则每轮的时间可由公式**错误!未找到引用源。**计算

$$T_i = \frac{V_i}{L} = \frac{R \cdot T_{i-1}}{L} = \ldots = \left(\frac{R}{L}\right)^i \cdot T_0 \tag{2}$$

令 $\lambda = R / L$，又 $T_0 = M / L$，所以可得迁移的总时间为

$$T_{total} = \sum_{i=0}^{n} T_i = \frac{M}{L} \cdot \frac{1-\lambda^{n+1}}{1-\lambda} \tag{3}$$

可以发现，虚拟机内存的大小直接影响了迁移时间的长短，而迁移时间越短，源主机上网络流量减少的速度也越快。因此，内存大小是决定该虚拟机是否应该被迁移的一个重要条件。

其次，虚拟机发送的流量是直接影响网络是否拥塞的重要因素。将消耗带宽最大的虚拟机迁移，可以最快地解决网络拥塞，但是需要考虑该虚拟机由攻击者控制的情况。即使进行迁移，该虚拟机在其他主机上仍然会继续发起 DoS 攻击，对整个云平台没有起到防御的作用。所以，迁移虚拟机时，流量状况也是重要的取决因素。

本文提出一种基于流量阈值的虚拟机选择方法，具体做法如下。主机 S 上虚拟机 i 内存大小为 $RAM(i)$，t 时刻产生的流量率为 $T_{ff}(i,t)$，虚拟交换机 j 的上行链路带宽为 B_j，门限阈值 α 由云服务提供商设置，当虚拟机 i 在 t 时刻的流量率满足 $T_{ff}(i,t) \le B_j \cdot \alpha$ 时，将其加入到待迁移序列中。令待迁移虚拟机集合为 I_t，则

$$I_t = \{i \mid T_{ff}(i,t) \le B_j \cdot \alpha, i \in S\} \tag{4}$$

即拥塞发生时，流量率低于阈值的所有虚拟机。对于集合 I_t 中的元素，再令

$$L_{i,t} = \frac{RAM(i)}{T_{ff}(i,t)} \tag{5}$$

将 $L_{i,t}$ 按照大小，升序排列，得到迁移顺序列表。每次从队列头部依次往后选择虚拟机进行迁移，一段时间后，重新检测网络状态，若拥塞依然存在，继续上述操作，直到云环境中服务恢复正常。

4.2　迁移触发机制的选择

本节首先从最简单的情形进行分析，即对单个虚拟机进行的迁移[8]。为方便分析，假设时间是离散的，即可以被分解为若干个个时间帧，每帧表示 1 秒。云服务提供商承担虚拟机迁移产生的开销，记为 $C_m t_m$，其中 C_m 是单个虚拟机单位时间内的迁移开销，t_m 是总的迁移时间。当网络发生拥塞时，由于服务质量无法得到保障，服务商将违反 SLA，并且需要为此进行赔偿，将这一部分的开销记为 $C_s t_s$，C_s 是单位时间内违反 SLA 的开销，t_s 是持续时间。不失一般性，本文定义 $C_m = 1, C_s = k$，

其中 $k \in R^{+}$ 。

设虚拟机总的迁移时间为 T ，且认为迁移结束时网络拥塞即得到解决。云平台在时刻 v 检测到网络中出现拥塞，需要确定一个迁移的开始时刻 t ，使得总的开销最小。定义一个开销函数 $C(t)$，包括迁移成本以及由于违反 SLA 产生的开销。由上述描述，可以得到如公式的开销函数。

$$C(t)=\begin{cases} T\cdot C_m & 当t<v,v-t\geq T; \\ T\cdot C_m+(t-v+T)\cdot C_s & 当t<v,v-t<T; \\ T\cdot C_m+(t-v+T)\cdot C_s & 当t\geq v. \end{cases} \tag{6}$$

开销函数描述了三种情形，包含了 t 和 v 之间可能的关系。将上式中的三种情形分别表示为 C_1,C_2 和 C_3，C_1 描述的情形是虚拟机迁移发生于产生拥塞之前，且迁移结束后仍未检测到网络拥塞，因此开销仅包括虚拟机迁移产生的费用。C_2 表示迁移开始于拥塞之前，但网络拥塞时迁移仍在进行。C_2 包含两部分：(a) 虚拟机迁移产生的费用；(b) 拥塞时违反 SLA 的开销。C_3 表示网络检测到拥塞后，开始虚拟机的迁移，开销情况同 C_2 。

容易发现，C_1 下的开销最小。需要指出的是，这个最优解是在离线分析的条件下得到的，即总是可以预先判断拥塞发生的时刻，并在此之前进行虚拟机的迁移。然而，这样的假设对于网络中的攻击场景来说是难以成立的，因为网络空间中基于未知漏洞和后门的未知攻击随时可能发生，先验知识不足以保证云环境的安全或对攻击进行防御。

但这给本文提供了一种解决思路，即在线条件下，应当尽量在网络产生拥塞之前，或者拥塞刚刚发生时触发虚拟机迁移，这样可以使得总的开销最小。需要注意的是，要避免由于瞬时峰值触发的迁移，而且网络负载呈现下降趋势时也不必进行迁移。

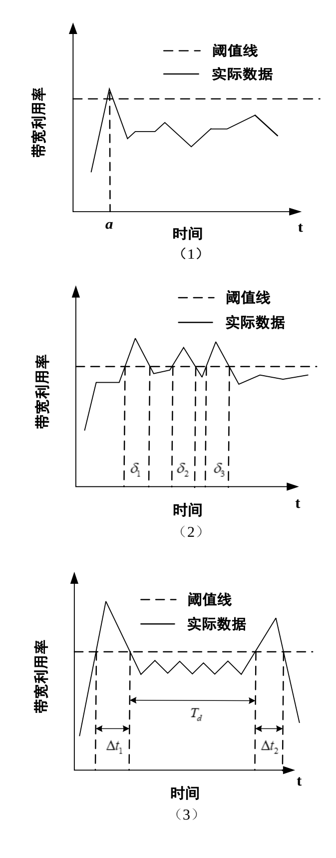


图 4　带宽利用率随时间变化的三种可能情形

如图 4 中(1)所示，a 点出现瞬时峰值后，带宽利用率降低到阈值线以下，此时不应该触发迁移。因此，本文设定一个度量值 δ ，表示带宽利用率超过阈值的时间占总的观测时间的比例，称之为过阈度。设置一个标准值 δ_{std} ，为系统允许的过阈度最大值，只要当真实的过阈度 δ_t 满足 $\delta_t > \delta_{std}$ 时，执行迁移操作。考虑到图 4 中(2)所示的情况，即在一段时间内，超过阈值的持续时间可能是分段的，且每段的过阈度都小于 δ_{std} ，但是此时网络状态已经接近于拥塞，应该进行虚拟机迁移。于是将触发时刻修改为第一次观测到总的超过阈值时间占观测时间的比值超过 δ_{std} ，即当 $\sum_{t=1}^{n-1}\delta_t < \delta_{std}$ 且 $\sum_{t=1}^{n}\delta_t \geq \delta_{std}$ 时，在第 n 次过阈度达到 $\delta_{std}-\sum_{t=1}^{n-1}\delta_t$ 时，触发迁移。还需要注意的是如图 4 中(3)的情形，当带宽利用率低于阈值线的时间较长时，上个持续时间 Δt_1 转化而来的过阈度，对于总的过阈度的影响必然是衰减的，所以 Δt_1 在经历时间 T_d 后，其衰减为 $\Delta t_{1\to T_d}=\dfrac{\Delta t_1}{e^{T_d\cdot\varphi}}$，其中 φ 为调节参数，是一个固定值，过阈度以衰减后的时间计算。

综合以上的条件及限制，本文对触发迁移的策略选择如下：将所有衰减后的过阈度值相加，在第一次超过标准值时，触发迁移，直至带宽利用率回归稳定的正常水平；然后将过阈度和观测时间清零，重复上述过程。

4.3　迁移目的地的选择

由于本文主要解决是网络流量出现的拥塞情况，因此在选择迁移的目的主机时，按照主机的带宽利用率进行升序排列，每次选择队首的主机作为迁移的目的主机，一次迁移完成后，对主机队列进行更新，并重复上述过程。

5　仿真结果分析

设置云环境中有 100 个物理主机，其带宽资源均为 120。每个主机上虚拟机数量服从[5,10]的均匀分布，虚拟机所需的带宽资源服从[1,20]的均匀分布，将各个虚拟机内存大小进行归一化处理，使其满足[1,3]的均匀分布。假设虚拟机带宽每个时间单元变化一次，且迁移过程均可在一个时间单元内完成。则 50 个时间单元内，各个主机的带宽需求总和如图 5 所示。

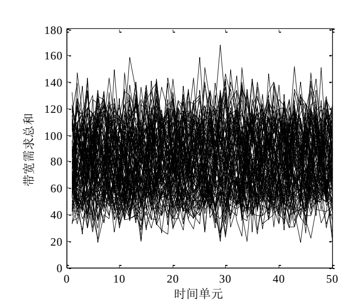


图 5　所有主机的带宽需求总和随时间的变化情况

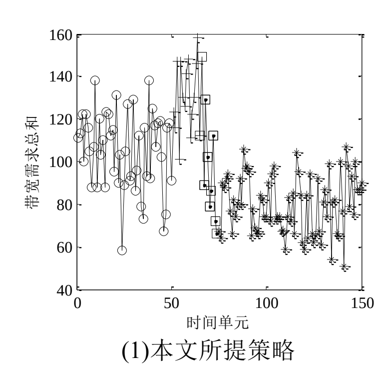
经统计可以得到，每个时间单元内，带宽需求总和大于 100 的主机比例约为 0.2，大于 120 的比例约 0.05。本文将过阈度的

标准值 δ_{std} 设置为 0.3，门限阈值 α 为 0.25。

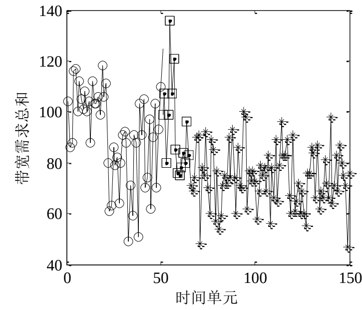
*<I, NA>*情形中，攻击者选择任一虚拟机数量最多的主机进行攻击，由于攻击流量过小，DoS 效果不明显；过大则可能被系统关闭而禁止服务，因此假设发送流量为 30。此时，基于本文所提的虚拟机迁移策略，阈值设置为 120 时可得到该主机带宽需求与时间单元的关系如图 6（1）所示。圆圈部分（图中用 o 表示）为第一阶段主机上承载 10 个虚拟机时的带宽需求变化情况，此时迁移未被触发；十字部分（用+表示）为攻击者实施攻击的阶段，因为主机本身带宽资源已接近饱和，所以这种攻击可以达到迅速形成 DoS 的效果；从方形部分（用□表示）开始，由于触发了迁移机制，开始对主机上的虚拟机进行迁移；根据每次迁移后主机的带宽需求判断是否继续进行迁移，直至星形部分（用*表示）出现，表示主机上拥塞已得到缓解。仿真结果表明，该情形下迁移的虚拟机平均数量为 3.08 个。

图 6（2）是基于 OpenStack 默认迁移机制下的带宽需求变化趋势，即只要带宽需求超过阈值，就将内存最大的虚拟机迁移到其他服务器上。对比图 6（1）可以发现，在攻击者发起攻击之前，该策略已经触发了虚拟机迁移；攻击时也因为带宽需求总和过大而进行了迁移操作。这种策略的优势在于对 DoS 攻击的响应速度更快，减轻攻击影响的效率更高。然而其缺点也很明显：没有考虑瞬时峰值，会产生很多不必要的迁移；平均迁移数量为 3.36 个，迁移成本更高。

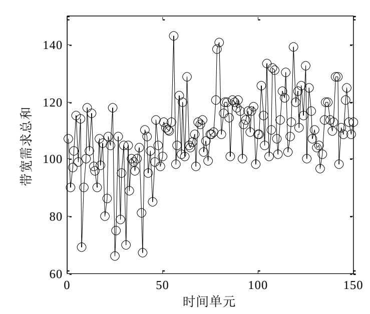
基于文献**错误!未找到引用源。**提出的博弈策略，可以得到如图 6（3）所示的带宽需求变化。该策略在发生网络拥塞时，限制每个虚拟机的最大发送流量，例如降低为 90%，若需求仍然超过资源总量，则进行丢包处理。该策略优势只需要设定防火墙阈值和丢包规则，没有迁移成本，是三种策略中开销最小的。但是这种方法并不能有效解决攻击者造成的 DoS 攻击，反而因为流量限制影响了正常用户的使用，甚至违反 SLA。



(1)本文所提策略

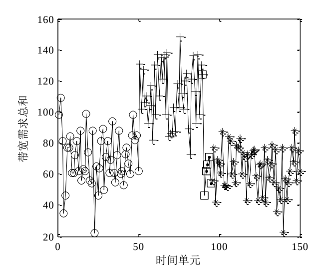


(2)OpenStack 默认迁移机制

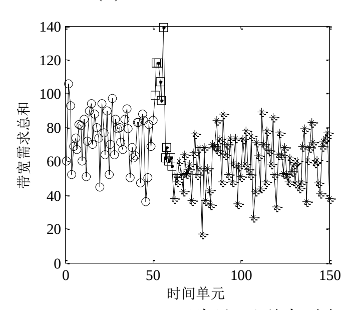


(3)基于博弈的迁移策略

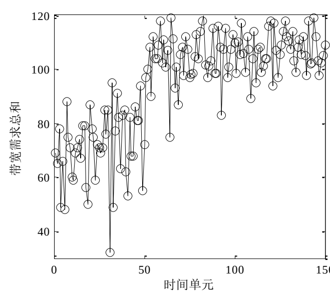
图 6　*<I，NA>*模型下带宽需求总和随时间的变化情况



(1) 本文所提策略



(2) OpenStack 默认迁移机制



(3) 基于博弈的迁移策略

图 7　*<NI，A>*模型下带宽需求总和随时间的变化情况

*<NI, A>*指的是攻击者对任一主机发起攻击，且恶意流量可实现自我调节，使得虚拟机不会被判定为实施恶意行为。假设恶意流量的调节范围为[20,40]，图 7（1）为主机上运行 7 个虚拟机，阈值设置为 120 时带宽需求随时间的变化情况。可以发现，由于攻击前带宽需求不高，而且攻击者的流量是动态变化的，因此十字阶段（图中用+表示）持续较长时间，才达到触发迁移的条件。尽管可能对正常用户的服务造成一定的影响，但这种策略是在避免瞬时高峰、尽量减小迁移次数和缓解 DoS 攻击二者中做出的权衡，更具有实用意义。此时，平均迁移数量为 1.01。

由于服务器上虚拟机数量较少，攻击前带宽需求小，所以图 7（2）中开始阶段与图 7（1）无明显区别；攻击发生时，触发虚拟机迁移，带宽需求随之降低。此时，虚拟机平均迁移数

量为 0.97 个，略低于本文策略。综合来看，OpenStack 默认策略在带宽需求小时缓解 DoS 攻击的效果与本文策略接近，但在带宽需求大时不宜采用默认策略，容易产生不必要的开销。

图 7（3）由于对带宽需求进行了限制，可以发现总和处于一个较稳定的水平。但实际上，用户的正常服务受到了较大影响，是一种对 DoS 攻击的妥协方法，没有从实际角度缓解 DoS 攻击带来的性能降低和安全隐患。真实网络环境下不宜采用。

图 8 表示在<*NI*，*A*>情形，设定不同阈值时，需要迁移的虚拟机数量与主机上虚拟机数量之间的关系。易知，相同阈值条件下，主机上虚拟机数量越多，缓解 DoS 攻击时需要迁移的虚拟机数量也更多；而对于同一主机，阈值越低，需要迁移的虚拟机数量越多。因为阈值低时，只有迁移更多数量的虚拟机，才可以使得带宽需求降低到阈值线以下，对于 DoS 攻击防御的效果更好，但更多的迁移也使得开销增加。

对于另外两种情形<*I*，*A*>、<*NI*，*NA*>，仿真的结果只是在迁移的触发时刻（即方形部分□起始位置）和迁移的虚拟机数量上有所区别，利用虚拟机迁移都可以减轻攻击行为造成的主机 DoS，且本文策略相较于其他两种策略，能适应于不同的攻击者行为，以可接受的迁移开销，快速缓解 DoS 攻击造成的威胁。

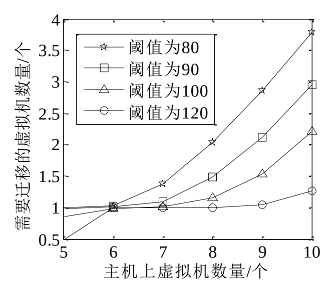


图 8　<*NI*，*A*>模型下，阈值不同时迁移的 VM 数量与主机上 VM 数量的关系

6　结束语

云环境资源共享的模式使得不同用户的虚拟机可以共存于同一物理主机上，攻击者可以利用恶意虚拟机持续消耗带宽，造成其他用户正常服务受到影响，形成云平台中的 DoS 攻击。利用虚拟机迁移，在设定的触发机制下，将发生 DoS 攻击的主机上特定的虚拟机迁移到其他可以提供正常服务的主机上，一方面保证虚拟机服务的正常运行，同时缓解源主机上的 DoS 攻击。实验结果表明，虚拟机迁移可以在较短的时间内，有效抵御 DoS 攻击，迁移产生的开销可以随云服务提供商设置的阈值变化，即 QoS 要求越高，迁移开销越大。今后可以结合人工智能的相关技术，对攻击流量的特征进行识别、提取，直接对攻击者进行限制，减小迁移操作带来的开销。

参考文献：

[1] Ristenpart T, Tromer E, Shacham H, *et al.* Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds [C]// Proc of the 16th ACM Conference on Computer and Communications Security. New York: ACM Press, 2009: 199-212.

[2] 刘孟. 云环境下 DDoS 攻防体系及其关键技术研究 [D]. 南京: 南京大学, 2016. (Liu Meng. Architecture of DDoS Defense in Cloud Environment and Its Key Technologies [D]. Nanjing: Nanjing University, 2016)

[3] Bedi H S, Shiva S. Securing cloud infrastructure against co-resident DoS attacks using game theoretic defense mechanisms [C]// Proc of International Conference on Advances in Computing, Communications and Informatics. New York: ACM Press, 2012: 463-469.

[4] Qiao Yan, Yu F R. Distributed denial of service attacks in software-defined networking with cloud computing [J]. IEEE Communications Magazine, 2015, 53 (4): 52-59.

[5] Zhang Tianwei, Lee R B. Host-Based Dos Attacks and Defense in the Cloud [C]// Hardware and Architectural Support for Security and Privacy. New York: ACM Press, 2017.

[6] Moon S J, Sekar V, Reiter M K. Nomad: mitigating arbitrary cloud side channels via provider-assisted migration [C]// Proc of the 22nd ACM Conference on Computer and Communications Security. New York: ACM Press, 2015: 1595-1606.

[7] 赵硕, 季新生, 毛宇星, 等. 基于安全等级的虚拟机动态迁移方法 [J]. 通信学报, 2017, 38 (7): 165-174. (Zhao Shuo, Ji Xinsheng, Mao Yuxing, *et al.* Research on dynamic migration of virtual machine based on security level [J]. Journal on Communications, 2017, 38 (7): 165-174.)

[8] Wang Huandong, Li Yong, Zhang Ying, *et al.* Virtual machine migration planning in software-defined networks [C]// Proc of International Conference on Computer Communications. 2015: 487-495.

[9] Beloglazov A, Buyya R. Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers [J]. Concurrency and Computation: Practice and Experience, 2012, 24 (13): 1397-1420.